金融区块链

下一场金融革命

深圳前海瀚德金融科技研究院◎组编
曹彤◎主编

FINANCE
BLOCKCHAIN

- 未来的金融世界会呈现哪些颠覆性改变?
- 为什么互联网金融并非最终的创新模式?
- 为什么说人类社会终将重返自金融时代?

区块链助力自金融的发展
引领可编程经济体的到来

机械工业出版社
CHINA MACHINE PRESS

金融区块链

下一场金融革命

深圳前海瀚德金融科技研究院◎组编
曹彤◎主编

机械工业出版社
CHINA MACHINE PRESS

本书通俗易懂地介绍了区块链技术在金融领域的应用范围、实践案例和未来趋势。在讲述技术理论的同时，汇集了大量成功案例，从共识、信任和智能金融这三个角度由浅入深地向读者介绍了区块链的由来与发展，区块链的去中心化、分布式账本、智能合约、智能社会的技术原理和特征，区块链在金融业的应用前景以及对区块链的展望与畅想等，引领读者走进并读懂金融区块链的世界。

本书对区块链如何帮助银行、证券、保险、资产管理公司和第三方服务机构等金融机构构建更加高效和智能的基础架构做了详细阐述，助力自金融的发展，引领可编程经济社会体的到来。作为一本金融区块链的科普读物，本书适合普通金融从业者及对新金融感兴趣的读者阅读。

图书在版编目（CIP）数据

金融区块链：下一场金融革命/深圳前海瀚德金融科技研究院组编；曹彤主编. —北京：机械工业出版社，2017.5

ISBN 978-7-111-56751-6

Ⅰ. ①金… Ⅱ. ①深…②曹… Ⅲ. ①电子商务—支付方式—应用—金融 Ⅳ. ①F83

中国版本图书馆 CIP 数据核字（2017）第 097244 号

机械工业出版社（北京市百万庄大街 22 号　邮政编码 100037）

策划编辑　康会欣

责任编辑　康会欣　孙东健

封面设计　高鹏博

北京顶佳世纪印刷有限公司印刷

2017 年 6 月第 1 版 · 第 1 次印刷

170mm×242mm · 11.5 印张 · 165 千字

标准书号：ISBN 978-7-111-56751-6

定价：39.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部负责调换

电话服务	网络服务
社 服 务 中 心：（010）88361066	教 材 网：http://www.cmpedu.com
销 售 一 部：（010）68326294	机工官网：http://www.cmpbook.com
销 售 二 部：（010）88379649	机工官博：http://weibo.com/cmp1952
读者购书热线：（010）88379203	**封面无防伪标均为盗版**

编辑委员会

前言

一、区块链是推动金融业代际跃升的重要力量

2014 年 10 月，在比特币备受各国央行打压之时，大英图书馆举行了一场关于比特币未来的研讨会。在会上，比特币的底层技术——区块链，引起了人们的兴趣。这项有趣的技术，可广泛应用于政府治理、公共管理、金融交易、资产公证等领域。自此，区块链正式从幕后走向前台，进入了更多创新人士的视野，并迅速在全球范围内掀起研究热潮。

区块链技术在经历了最早仅应用于比特币等数字加密货币的 1.0 阶段之后，开始迅速向金融与智能商业合约的 2.0 阶段挺进。银行、证券、保险等传统金融机构以及其他更广泛的商业机构都可以与区块链结合，产生创新应用场景。尽管如此，区块链技术仍然处于发展的早期阶段，面临着种种局限性和不确定性。然而，就如同 20 年前的互联网技术一样，重重困难也难掩其价值。区块链在中国日新月异的发展当中，最重要的价值就是推动金融业的发展与创新。由于互联网金融的快速扩展已持续了 20 年，其显现出的问题仅靠互联网本身难以化解，需要更新一代技术来满足社会各方对金融服务日新月异的要求。区块链技术由于其去中心化、不可篡改、共识性、匿名性、自治性和开放性等特性，能够帮助传统金融业在很大程度上降低成本，提高安全性，扩展金融的业务和从业者范围，提升客户体验。区块链技术将会成为

推动金融业代际跃升的重要力量，为我们开启下一代金融革命，引领金融业进入全新时代。

二、区块链帮助金融业提高共识

在区块链的世界里，任何一条交易都需要通过网络广播出去，只有获得了一定数量节点的认可之后才能写入。这样的安排可以确保任何被写入区块链的信息都是取得了共识的，被足够多的节点共同认可的，其真实性和有效性会在更高维度上得到保障。尽管互联网技术是为解决信息不对称而生的，但这些大量的、碎片化的信息真真假假，其中混杂着海量的无用和失真信息，形成信息的二次不对称性。在区块链网络中，只有达成共识的信息才被写入，无用和虚假信息会被自动拒绝。在金融业，很多欺诈和违约是由于信息不对称造成的，例如资产重复抵押、虚假身份验证等。区块链技术能够帮助金融业建立更广泛的社会共识机制，降低金融业的风险，提高其安全强度。

三、区块链推动金融业诚信系统构建

区块链技术建立的数据库是基于时间序列的不可篡改的信息记录。由于区块链网络中引入了工作量证明机制，它在现有的基于评级模型的金融系统之外另辟蹊径，开创了无须第三方信用背书的基于区块链的金融网络，有效地解决了自证其信的问题。区块链网络用自身的技术特征杜绝了人为因素，从而成为真实有效的征信系统的基础。金融机构可以将企业征信、个人征信、第三方增信系统引入区块链技术。此外，在客户数据库的客户身份验证、反洗钱反欺诈方面，区块链也能够帮助金融机构降低风险和合规成本。在建立诚信金融、诚信社会的过程中，区块链将是减少信任成本、削弱市场摩擦的利器。

四、区块链推动金融进入智能合约时代

现有的金融系统是依靠人来操作的。区块链智能合约为通往新型的自动化、数字化合约目标铺设了一条道路。智能合约将现有的传统合约迁移至区块链网络，条款以事先植入的计算机算法的形式存在，同时通过接入外部可信数据库，自动触发和执行后续操作。智能合约首先得以在标准化的简单合约中推行（例如金融衍生品合约），之后可以尝试在更广的范围内试行。智能合约可以帮助金融机构杜绝人为失误，有效记录事实，清晰划分责任和义务，并自动触发合约的执行，其实质是促进金融服务的个性化，催生“小众规模化”全新模式。

五、区块链将开启自金融时代

人类社会的早期金融形态就是一种“自金融”形态，即每一个个体都是金融主体。随着工业化的发展，集中化与专业化成为社会的主要形态，金融业则表现为以金融机构为核心的间接金融体系。随着互联网成为社会生活的底层通用技术，分散化与多元协作化日益成为社会发展的主流取向，Uber 与 Airbnb 等模式是典型代表。区块链技术无疑是在这一趋势下出现的一个助推器。互联网技术在“去中心化”的同时却创造了新的中心，严格意义上与“互联网精神”相悖，但在区块链叠加到互联网技术上之后，则有可能创造真正的多中心。这些多中心在社会学属性上具有自治性，在金融业态上则表现为真正的“自金融”，一种超越信息不对称性的全新金融业态。人类社会几千年的演绎，终因技术发展而螺旋式重回“自金融时代”。金融的效率性、安全性及营利性将达成一种更高水平的平衡。

从这个意义上说，我们不能仅将区块链视为一种信息技术，因为它将构

成一个全新的时代。400 年来，现代金融始终在构筑和强化中心化的体系，体系的中心是那些工业制造强国和国际贸易强国，我国一直处于边缘和跟跑地位。21 世纪，人类社会明显进入技术和数字时代，金融体系开始由技术元素和数字强国主导，这一趋势已由互联网金融所证明。展望未来，我们有理由相信，今天耳熟能详的“互联网金融”，将会很快迭代为“区块链金融”，并将进一步演绎为“自金融”。从这个意义上看，我国的区块链实践关乎全球金融体系的重构，关乎全球金融模式与发展轨迹，更关乎中国在全球的金融地位与价值贡献。

为此，每一位金融从业者都应高度关注区块链和其他全新的数字技术，关心金融科技，并勇于实践。

目录

第 1 章　区块链开启新金融时代

1.1　金融界风云突变

在过去的几个世纪里，各国都在以中央集权的方式发行货币。东方国家垄断货币发行权，更是有将近两千年的历史。中国西汉时期，汉武帝为了加强中央集权，推行了包括统一铸币在内的一系列经济政策。此后，虽然朝代更迭，这些垄断经济政策却一直被延续了下来。明清时期，官方更是推行了“海禁”来阻止非官方贸易。货币在全球范围内都被国家集权所垄断，各国货币通过法定含金量来体现价值。

从 1971 年美元放弃金本位制开始，全球货币进入了一个新的阶段，彻底放弃了与金银的内在联系，也不再受到金银数量有限的限制，以国家主权信用担保的“信用货币”成为货币发展史上的一大深刻转变。自此，国家主权信用货币失去了掣肘，以美国为代表的许多国家进入了疯狂印钞的时代，只要经济出现问题，就开启一轮量化宽松政策，开启印钞机，加大货币供应量。而就是这日夜不停哗哗作响的印钞声，为经济危机埋下了巨大的隐患。

随着人类经济活动的发展，演化出一种新的资金融通活动，称作“金融”。人们将自己暂时用不到的闲置财富，借给急需消费或者生产的人，将资源再配置，以提高财富的有效利用度和社会产出。相对于需要借贷双方相识并且互相信任的直接融资方式，将资金交给信任的金融中介的间接融资方式更被人所青睐。居民将自己的存款存入银行，借款人通过银行将这笔存款贷出并用于消费或生产，而这笔钱最终又会被转化为存款，银行吸收存款后可

以再次放贷。这样一来二去，杠杆被放大到若干倍，人们不断透支未来的资产，用于现在的需求。但是，一旦产生过度信用消费，银行将会产生大规模的不良贷款，进而引发系统性金融风险。例如2008年的国际金融危机，次级抵押债券泡沫破裂，风险全面爆发，引发了雷曼兄弟、美林、AIG等美国金融巨头的破产和收购事件，其中既有金融机构滥用金融衍生品杠杆的原因，也有美国政府低利率货币政策的推波助澜。在危机面前，货币信誉、社会和经济的稳定面临严峻挑战，政府又不得不出面挽救“大而不能倒”的银行。为了救市，政府只好继续扩大货币投放，但不良贷款仍在，货币总量处于失控的边缘。

货币发展至今，在给人类带来了巨额财富的同时，也为社会的发展埋下了隐患。“信用”这个伟大的经济发现，仿佛一剂毒药，让人类欲罢不能。在资本主义教条下，人们相信经济这块蛋糕会无限地增长，中心化的政府和银行为了满足自身要求而疯狂地开动印刷机，而真正能够救市的却是科学家。每过一段时间，就会涌现出一些科学发明，其创造的新产业所产生的经济效益刚好被用于购买政府从2008年以来凭空创造出来的几万亿美元的账单。可以说，科学创新和经济泡沫增长是一场令人担忧的赛跑。

2008年的这场国际金融危机堪称百年不遇的巨大危机，其阴影延续至今，使资本主义世界范围内的经济长期低迷，财富分配愈发不均匀，社会矛盾尖锐，不安定因素层出不穷。不世之材中本聪（Satoshi Nakamoto）表达了他对金融危机的愤怒：“常规货币的根本问题是维持其运作所必需的信任。人们必须信任央行不会让这种货币贬值，但是不兑换纸币的历史则充斥着对这种信任的背弃。”也正是这位神秘人物，创造了比特币和区块链，又在多年后引发了全世界对于区块链的思考，将飞速前进的科技与金融巨轮联系在一起，推动经济走向新的轨道。

1.2 比特币横空出世

1.2.1 应运而生

2008年11月1日，中本聪坐在电脑前，最后审视着自己的杰作——一篇题为《比特币：一种点对点的电子现金系统》的论文。随着他点击了发送键，一封标题为“Bitcoin P2P e-cash paper”的邮件悄悄进入metzdowd.com网站的密码学邮件组。深夜，星光熠熠，熟睡中的人们并不知道，一个新的时代已经拉开序幕，比特币和区块链这一对孪生兄弟已悄悄登上了历史舞台。

中本聪在他的论文中敏锐地提出，目前互联网上的贸易内生性地受制于“基于信用的模式”（Trust-based Model）的弱点，也就是在物理现金缺失的情况下产生的销售费用和支付问题上的不确定性。因此，买卖两方都不得不借助金融机构作为可信赖的第三方信用中介。然而，第三方信用中介的存在，不仅增加了交易的成本，还限制了实际可行的最小交易规模以及很多本身无法退货的商品和服务的交易。这一段论述一针见血地指出了信息革命以来电子商务的重大问题——信用。事实上，自2008年开始的严重经济危机在很大程度上正是始于金融机构对借贷方信用的评估失准。

针对上述问题，中本聪在论文中详细解释了他的解决方案——一个基于密码学原理而非信用的电子支付系统。按照中本聪的设想，这个系统通过点对点分布式的服务器来生成依照时间先后排列并记录的电子交易证明，从而杜绝肆意篡改支付交易的可能，在任何达成一致的双方之间直接进行支付，不再需要第三方中介参与。中本聪设计的系统使用密码来背书，使得在互相完全不信任的双方之间进行的交易也能得到安全保障。他首先提出了“电子货币”的概念，定义为如图1-1中所示的一串数字签名。

按照中本聪的描述，电子货币的每一位拥有者都要在这枚电子货币的末尾签署一个数字签名，这个签名是由哈希函数生成，并使用下一位拥有者的

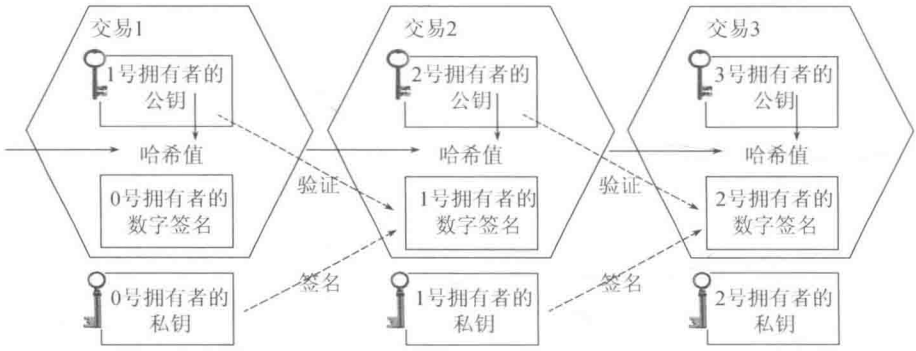

图 1-1 中本聪对电子货币概念的阐释示意

公钥（Public Key）来加密的。在将数字签名附加在这枚电子货币的末尾后，它就可以被发送给下一位所有者了。收款人使用自己的私钥对签名进行解密，得到哈希值之后对内容的真实性进行检验，就能够验证上一位所有者的身份。这样一来，图 1-1 中的每一次交易就形成了一组以“区块”（Block）存在的数据。

其实，公钥加私钥的数字加密方法早在 1976 年就由斯坦福大学的迪菲（Diffie）和赫尔曼（Hellman）两人提出，但是上述支付过程存在着致命的缺陷，这种缺陷被称为“双花问题”（Double-spending Problem）。顾名思义，就是某一枚签名被同一名付款人发给两个甚至多个收款人的情况。这也是基于数字加密的电子支付系统长时间少有人问津的主要原因之一。针对这个问题，中本聪为系统本身设计了保障交易的时间序列机制，即“时间戳服务器”（Timestamp Server）。他在每个区块中增加了一个仍然是由随机散列生成的时间戳字符串，并要求支付者将该随机散列在全网广播。这样一来，支付系统网络上的所有参与者都能够证实某一串数据在某一个时刻必然是存在的。下一位拥有者在使用这枚数字货币时，同样要生成一个时间戳，并且这个时间戳将前一个时间戳纳入其随机散列值中，每一个随后的时间戳都对之前的时间戳进行增强，这样就形成了一个公开、透明的时间序列链条。

对于这个拥有了时间序列的系统，中本聪仍然不完全满意。为了保证这

个链条上的信息是不可更改的，他又引入了“工作量证明”（Proof of Work）机制，在区块中补增一个随机数（Nonce），使得该给定区块的随机散列值以一个或多个0开始，随着0的数目的上升，找到这个解所需要的工作量将呈指数增长，但是检验结果仅需要一次随机散列运算。当某个节点想要生成一个区块时，它必须通过反复尝试来找到这个随机数，直到找到为止。这将耗费很高的CPU工作量，除非重新完成相当的工作量，否则该区块的信息不可更改。

短短2个月之后的2009年1月3日，比特币客户端程序正式面世。中本聪进行了首次挖矿（Mining），并且获得了首批50个比特币，同时创造了第一个区块，称为“创世纪区块”，当中记载了这样一句话：“*The Times* 03/Jan/2009 Chancellor on brink of second bailout for banks（《泰晤士报》：2009年1月3日，财政大臣正处于实施第二轮银行紧急援助的边缘）。”当时正是英国的财政大臣达林被迫考虑第二次出手纾解银行危机的时刻，这句话是《泰晤士报》当天的头版文章标题。为什么中本聪要在创世纪区块上写入这个新闻标题，多来年一直争议不断，但是人们普遍推测，中本聪将新闻标题写入创世纪区块的目的不仅仅是为它打上时间戳，更是为了纪念这一货币史上具有转折意义的重要时刻。

比特币在运行之初像一个酷炫的淘金游戏。玩家只要下载一个特殊的应用程序即可开始，一旦进入比特币网络，玩家就是一个“矿工”，只要贡献出CPU的运算能力，就可以参与“挖矿”了。“挖矿”的过程好像是一个数学解密游戏，需要通过哈希现金（Hash Cash）算法解出答案。哈希现金是一个有无穷多个解的方程，但在这个解密游戏当中，只有一个解是对的，并且没有人知道正解究竟是哪一个。于是我们的比特币玩家只好一个一个地实验，直到找到正确答案。但是，比特币网络中有非常多的玩家，他们都同时在玩这个游戏，先解出正解的才是赢家。这个游戏会持续多久呢？平均大约需要10分钟。如果玩家的运算能力越来越强，挖矿时间越来越短，比特币网络会根据算法调节难度，使挖矿时间加长，反之则减小难度，使时间变短，从而

保持一个精妙的平衡。10 分钟后，获胜的玩家因为成功解出哈希函数而获得若干比特币和这几分钟内的数据块打包权，玩家可以将这期间的交易数据打包成为一个区块，连接在上一个区块之上，成为一个数据链条，称为区块链。没有成功的玩家只好放弃之前的全部工作，继续投入下一轮挖矿之中。

随着比特币越来越热门，玩家的数量越来越庞大，在千军万马过独木桥的竞争当中，使用个人电脑的 CPU 进行挖矿慢慢没有了优势，甚至可能一年也挖不到一个区块。于是聪明的玩家们组成一个团体，将所有的电脑连接在一个由特定算法设计而成的服务器“矿池”上，大大加强了计算机的运算能力，挖矿的成功率也得到提升。一旦队伍成功挖出了新的区块，所获得的比特币奖励将按照比例进行分配。

比特币的总数在设计之初就被限定在了 2100 万枚，而作为挖矿奖励的比特币数额并不是固定不变的。从创世纪区块起，比特币以平均每 10 分钟 50 枚的速度增加，直到达到总数的一半，即 1050 万枚。之后挖矿所得比特币的数量减半，每 10 分钟为 25 枚，待剩余比特币总数的一半被挖出（即被挖出的比特币总量达到 1575 万枚）时，平均每 10 分钟挖矿所得会再次减半。到 2140 年左右，比特币将达到上限 2100 万枚。虽然比特币的总数固定，但随着挖矿难度的增加，单枚比特币的产值会逐级攀升，社会财富会不断增长，所以从长远来看，比特币是一种通缩货币。这也就避免了像魏玛共和国那样的通货膨胀和失业率飙高引起的经济大萧条等故事在比特币上上演。

1.2.2 蹒跚成长

比特币诞生后的一年里，只有一小批密码学爱好者对其比较关注。对于普通大众来讲，这还是一个陌生的“技术宅”名词，而第一次比特币交易也确实充满着“技术宅”的气息。2010 年 5 月 21 日，美国佛罗里达州的程序员 Laszlo Hanyecz 用 1 万枚比特币购买了价值 25 美元的比萨优惠券。这笔交易不仅填饱了 Laszlo 的肚子，也诞生了比特币第一个公允汇率：1 比特币 = 0.008 美元。

一个半月后，2010年7月11日，著名新闻网站Slashdot报道了比特币的新版客户端。该新闻为比特币带来大批新用户，使其仅仅在5天之后就升值了10倍。之后的发展可谓风生水起：2010年7月17日，第一个比特币平台Mt. Gox诞生；2010年11月6日，Mt. Gox上1枚比特币的价格达到0.5美元，比特币的经济规模达到100万美元；2011年1月27日，3个来自津巴布韦的账单在Bitcion-otc平台上用4枚比特币换取了100万亿津巴布韦币，成为迄今为止数额最大的比特币交易；2011年2月9日，比特币的价格首次达到了1美元/枚。

比特币与美元等价的消息被媒体大肆报道后引发了人们的高度关注。2011年4月，美国《时代周刊》和《福布斯》等权威期刊也相继发表了关于比特币的文章。越来越多的人投入到比特币玩家的行列，比特币与英镑、巴西币、波兰币的互兑交易平台先后开张。瑞典海盗党的创始人Rickard Falkvinge甚至宣布，他已经将自己所有的财产都换成了比特币，还借了很多钱以进一步囤积。

2011年6月8日，Mt. Gox上的比特币成交价格已经达到31.91美元/枚，然而就在这时，意外状况突然出现。6月19日，黑客从感染木马的电脑上盗用了用户的Mt. Gox证书，并利用自己创建的0.01美元订单大量买入比特币。此次袭击使6万个用户数据泄漏，造成总计875万美元的账户损失。Mt. Gox虽然宣布短期的价格异常变动无效，但被迫关闭交易7天来修复BUG。这一事件极大地刺激了全球的黑客们，此后几个月内多家比特币交易平台先后遭到攻击。11月14日，比特币价格又跌回了1.99美元/枚。

进入2012年，黑客仍然是比特币玩家挥之不去的噩梦。3月1日，比特币服务器超级管理密码泄漏，价值22.9万美元的46703枚比特币失窃。但是，随着9月15日伦敦比特币会议的召开、9月27日比特币基金的创立、11月25日欧洲第一次比特币会议的召开、12月6日首家在欧盟法律框架下进行运作的比特币交易所——法国比特币中央交易所的诞生等，这一系列高级别事件的发生使比特币即便在黑客阴影的笼罩下依然保持强劲的上涨态势。11月